UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,033	12/31/2003	Carlos J. Gonzalez	SNDK.281US0	3703

36257 7590 07/25/2006

PARSONS HSUE & DE RUNTZ LLP
595 MARKET STREET
SUITE 1900
SAN FRANCISCO, CA 94105

EXAMINER	
MASKULINSKI, MICHAEL C	
ART UNIT	**PAPER NUMBER**
2113	

DATE MAILED: 07/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/751,033	GONZALEZ ET AL.	
	Examiner	Art Unit	
	Michael C. Maskulinski	2113	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *21,22 and 25-27* is/are allowed.

6)☒ Claim(s) *1-4,10,17,18,20 and 23* is/are rejected.

7)☒ Claim(s) *5-9,11-16,19 and 24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/9/04;6/17/05;10/11/05*
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Non-Final Office Action

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-4, 10, 17, 18, 20, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Langford et al., US 2004/0205328 A1, and further in view of Smith et al., US 2004/0088534 A1.

Referring to claim 1:

a. In paragraph 0023, Langford et al. disclose that firmware and redundant firmware are stored in the same flash memory (flash memory containing at least first and second copies of firmware code stored in different locations therein). Further, in paragraphs 0018 and 0020, Langford et al. disclose a microprocessor, a read-only-memory (ROM) containing microprocessor accessible boot code and a random-access-memory (RAM) for storing microprocessor accessible firmware code.

b. In paragraph 0027, Langford et al. disclose that when boot code is executed within the memory, the boot code will check a flag, such as Pside validity flag to determine whether the image within Pside flash memory is valid. The validity flag is stored in a nonvolatile memory. Further, in paragraph 0038,

Langford et al. disclose that the validation may take the form of a cyclical redundancy check across the entire image (executing the boot code to transfer a first copy of the firmware from the flash memory to the RAM, identifying any bit errors in the transferred first copy of the firmware code).

c. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the validation may be performed using a CRC, but is not limited to that implementation. However, Langford et al. don't explicitly disclose that if bit errors are identified that are correctable, correcting the erroneous bits. In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to be able to correct at least single bit errors with the error correction codes. It would have been obvious to one of ordinary skill at the time of the invention to include the error correction codes of Smith et al. into the system of Langford et al. A person of ordinary skill in the art would have been motivated to make the modification because error correction codes are commonly included with data to correct single-bit errors and sometimes multi-bit errors. Including error correction codes in the firmware of Langford et al. would be an improvement because it would eliminate the need to switch over to a backup if simple correctable errors existed.

d. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form

the other firmware image (if bit errors are identified that are not correctable, reading at least a portion of the second copy of the firmware code into the RAM in place of at least a portion of the first copy containing the uncorrectable bit errors, and executing an error free copy of the firmware code from the RAM).

Referring to claim 2, in paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to be able to correct at least single bit errors with the error correction codes (wherein identifying any bit errors in the transferred first copy includes calculating error-correction-codes (ECCs) from individual portions of the first copy of the firmware by passing the firmware portions through ECC circuitry in succession as they are being transferred from the flash memory to the RAM, and comparing the calculated ECCs with ECCs previously calculated from said portions of the first copy of the firmware data).

Referring to claim 3, in paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to be able to correct at least single bit errors with the error correction codes. Since Smith et al. disclose error correction codes; it would be inherent to the system of Smith et al. to microprocessor executing an error correction algorithm of the boot code to correct erroneous bits.

Referring to claim 4, in paragraph 0047, Smith et al. disclose data elements within BIOS code and corresponding error correction codes associated with the BIOS code (wherein the individual portions of the first copy of the firmware code include one

or more sectors of data and an ECC previously calculated therefrom and stored in the flash memory therewith).

Referring to claim 10, in paragraph 0047, Langford et al. disclose that when boot code is executed within memory, boot code will check a flag, such as Pside validity flag to determine whether the image within Pside flash memory is valid (prior to executing the boot code to transfer a first copy of the firmware from the flash memory to the RAM, checking the state of a firmware present flag that is set when firmware is stored in the flash memory and continuing to execute the boot code to transfer the first copy of the firmware from the flash memory to the RAM only when the firmware present flag is set).

Referring to claim 17:

a. In paragraph 0023, Langford et al. disclose that firmware and redundant firmware are stored in the same flash memory (flash memory containing at least first and second copies of firmware code stored in different addressable locations). Further, in paragraphs 0018 and 0020, Langford et al. disclose a microprocessor, a read-only-memory (ROM) containing microprocessor accessible boot code and a random-access-memory (RAM) for storing microprocessor accessible firmware code.

b. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the validation may be performed using a CRC, but is not limited to that implementation. However, Langford et al. don't explicitly disclose storing at least first and second copies of firmware code in different addressable locations of the

flash memory by passing the firmware copies one at a time through the ECC circuitry and storing the ECCs calculated thereby in the flash memory. In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes. It would have been obvious to one of ordinary skill at the time of the invention to include the error correction codes of Smith et al. into the system of Langford et al. A person of ordinary skill in the art would have been motivated to make the modification because error correction codes are commonly included with data to correct single-bit errors and sometimes multi-bit errors. Including error correction codes in the firmware of Langford et al. would be an improvement because it would eliminate the need to switch over to a backup if simple correctable errors existed.

c. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the validation may be performed using a CRC, but is not limited to that implementation (thereafter initiating operation of the memory system by causing the microprocessor to execute the boot code to transfer the first copy of the firmware from the flash memory to the RAM) and it would be inherent to the system of Smith et al. to be able to calculate an ECC when transferring data to the RAM.

d. It would be inherent to the combined system of Langford et al. and Smith et al. to utilize the calculated and stored ECCs to identify any bit errors in the transferred first copy of the firmware code, and if bit errors are identified to be

correctable, causing the microprocessor to execute an error correction algorithm within the boot code to correct the erroneous bits, in order to result in the firmware code being loaded into the RAM without any errors.

e. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form the other firmware image (if bit errors are identified to be uncorrectable, transferring at least a portion of the second copy of the firmware code into the RAM in place of at least a portion of the first copy containing the uncorrectable bit errors, in order to result in the firmware code being loaded into the RAM without any errors).

Referring to claim 18, in paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes (wherein storing the firmware code includes storing ECCs individually calculated from one or more sectors of the firmware code).

Referring to claim 20, in paragraph 0047, Langford et al. disclose that when boot code is executed within memory, boot code will check a flag, such as Pside validity flag to determine whether the image within Pside flash memory is valid and in paragraph 0028, Langford et al. disclose that if on the other hand, Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system from the other firmware image (wherein storing the firmware code additionally includes setting a flag to indicate the presence within the flash memory of at least one firmware copy, and wherein executing

the boot code to transfer either of the first or second copies of the firmware code includes first reading the flag associated therewith and proceeding to read the copy of the firmware code only if the associated flag is set).

Referring to claim 23:

a. In paragraph 0023, Langford et al. disclose that firmware and redundant firmware are stored in the same flash memory (an array of flash memory cells storing data in charge storage elements and containing at least first and second copies of firmware code therein). In paragraphs 0027 and 0038, Langford et al. disclose that the validation of data may be performed using a CRC, but is not limited to that implementation. However, Langford et al. don't explicitly disclose having first and second sets of error-correction codes (ECCs) calculated from the first and second copies of the firmware code . In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes. It would have been obvious to one of ordinary skill at the time of the invention to include the error correction codes of Smith et al. into the system of Langford et al. A person of ordinary skill in the art would have been motivated to make the modification because error correction codes are commonly included with data to correct single-bit errors and sometimes multi-bit errors. Including error correction codes in the firmware of Langford et al. would be an improvement because it would eliminate the need to switch over to a backup if simple correctable errors existed.

b. In Figure 2, Langford et al. disclose a controller processor.

c. Circuitry that calculates ECCs from data passing through the circuitry would be inherent to Smith et al. since Smith et al. has ECCs.

d. Further, in paragraphs 0018 and 0020, Langford et al. disclose a read-only-memory containing boot code that the processor accesses and executes in response to initialization of the storage system and a random-access-memory that is accessible by the processor to obtain instructions to be executed.

e. In paragraph 0027, Langford et al. disclose that when boot code is executed within the memory, the boot code will check a flag, such as Pside validity flag to determine whether the image within Pside flash memory is valid. The validity flag is stored in a nonvolatile memory. Further, in paragraph 0038, Langford et al. disclose that the validation may take the form of a cyclical redundancy check across the entire image (wherein the boot code causes the processor to read the first firmware code copy including passing the read first firmware code copy through the ECC calculation circuitry which calculates ECCs and provides with respect to the first set of ECCs stored with the first firmware code copy a status with respect to any data errors existing in portions of the first firmware code copy to which the ECCs pertain).

f. In paragraphs 0027 and 0038, Langford et al. disclose that if the flag is valid, boot code will continue to boot the data processing system and that the validation may be performed using a CRC, but is not limited to that implementation ((A) if the status indicates that there are no data errors in a given

one of the portions of the first firmware code copy, thereafter writing the given portion of the first copy of the firmware code into the random-access-memory).

g. In paragraph 0047, Smith et al. disclose that the BIOS code includes error correction codes and it would be inherent to the system of Smith et al. to be able to correct at least single bit errors with the error correction codes ((B) if the status indicates that there are data errors in the given portion of the first firmware code copy, the boot code causes the processor to determine whether the number of bit errors in the firmware code exceed a given number, and (i) if the number of bit errors do not exceed the given number, further causes the processor to correct the erroneous bits and write the corrected first firmware code copy into the random-access-memory).

h. In paragraph 0028, Langford et al. disclose that if Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system form the other firmware image ((ii) if the number of bit errors is equal to or exceeds the given number, further causes the processor to read at least a portion of the second firmware copy).

i. In paragraph 0028, Langford et al. disclose that if, on the other hand, Pside validity flag indicates that microcode within Pside flash memory is invalid, boot code may then report a warning and will then continue to boot the computer system from the other firmware image. In this example, boot loader will check Tside validity flag for Tside flash memory. If this flag is valid, boot code will

continue to boot the data processing system using the images located in this flash memory (pass the read second firmware code through the ECC calculation circuitry which calculates at least one ECC therefrom and provides a status with respect to any data errors existing in said at least a portion of the second firmware code copy to which said at least one ECC pertains, and if the status indicates that there are no data errors in said at least one portion of the second firmware code copy, thereafter writing said at least one portion of the read second copy of the firmware code into the random-access-memory).

Allowable Subject Matter

3. Claims 5-9, 11-16, 19, and 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

4. Claims 21-22 and 25-27 are allowed.

5. The following is a statement of reasons for the indication of allowable subject matter.

Referring to claim 5, the prior art does not teach or reasonably suggest initially accessing a plurality of fixed locations in the flash memory one at a time until an initialization memory map is discovered to be stored at at least one of the plurality of fixed locations and that contains addresses of the different locations of the flash memory wherein said at least first and second copies of firmware code are stored,

reading data of the initialization memory map to obtain said addresses, and thereafter accessing the first copy of the firmware code.

Referring to claim 7, the prior art does not teach or reasonably suggest wherein the at least first and second copies of firmware code are stored in the different locations of the flash memory with only a given number of one or more bits of firmware code stored per flash memory storage element thereof, while the memory storage system is further characterized by storing user data in other locations of the flash memory with more than said given number of bits of user data per storage element thereof.

Referring to claim 9, the prior art does not teach or reasonably suggest identifying any bit errors in the transferred at least a portion of the second copy of the firmware code, and if bit errors identified in the transferred at least a portion of the second copy of the firmware code are not correctable, repeating the reading of said at least a portion of the second copy of the firmware code under conditions that tend to reduce the number of bit errors in the transferred at least a portion of the second copy.

Referring to claim 11, the prior art does not teach or reasonably suggest in response to identifying a number of bit errors of a predefined number of one or more, of setting a housekeeping flag associated with the locations of the flash memory from which the erroneous data of the first copy of the firmware are stored.

Referring to claim 19, the prior art does not teach or reasonably suggest wherein execution of the boot code by the microprocessor includes initially locating the map by accessing the predetermined plurality of locations one at a time until the map is found, and reading the contents of the map at the location where the map is stored.

Referring to claim 21, the prior art does not teach or reasonably suggest wherein the boot code causes the processor to access the plurality of predetermined addresses within the flash memory to locate and read the data of the memory map specifying addresses wherein one or more copies of the firmware are stored, thereafter reading the firmware code located at at least one of said specified one or more addresses and thereafter writing the read the firmware code into the random-access-memory.

Referring to claim 24, the prior art does not teach or reasonably suggest wherein the firmware code is stored in the flash memory with one-bit thereof per memory cell storage element, and further wherein data are stored at at least some of addresses of the memory array other than those containing the firmware code with more than one-bit thereof per memory cell storage element.

Referring to claim 25, the prior art does not teach or reasonably suggest (A) if the first flag is present and the second flag is not present, to proceed to load the firmware code into the random-access-memory, or (B) if both of the first and second flags are present, to provide access to the firmware code for testing without loading the firmware code into the random-access-memory, or (C) if the first flag is not present, neither attempt to load the firmware code into the random-access-memory nor attempt to provide access to the firmware code for testing.

Referring to claim 27, the prior art does not teach or reasonably suggest storing one bit of said at least first and second copies of the firmware code in individual storage elements of memory cells within said different locations of the flash memory and more

than one bit of said user data in individual storage elements of memory cells within said other locations of the flash memory.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The cited prior art is related redundant firmware and BIOS stored in a flash memory.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael C. Maskulinski whose telephone number is (571) 272-3649. The examiner can normally be reached on Monday-Friday 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert W. Beausoliel can be reached on (571) 272-3645. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael C Maskulinski
Examiner
Art Unit 2113